

FILED

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division**

2012 OCT 10 A 8:35

MICROSOFT CORPORATION, a
Washington corporation,
Plaintiff,

v.

Peng Yong, an individual;
Changzhou Bei Te Kang Mu Software
Technology Co., Ltd., d/b/a Bitcomm, Ltd;
John Does 1-3

Defendants.

Civil Action No.

1:12 CV 1004 GBL-IDD

FILED UNDER SEAL

COMPLAINT

Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges against Defendant Peng Yong, an individual; Defendant Changzhou Bei Te Kang Mu Software Technology Co., Ltd., d/b/a Bitcomm, Ltd, a Chinese company; and John Does 1-3; all controlling and/or facilitating the "Nitol" botnet and other illegal, malicious software ("malware") through approximately 70,000 sub-domains of the Internet domain known as 3322.org, set forth in Appendix A to this Complaint as follows:

NATURE OF ACTION

1. This is an action based upon: (1) The Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Common Law Trespass to Chattels; (3) Unjust Enrichment; (4) Conversion, and (5) Negligence. Microsoft seeks injunctive and other equitable relief and damages against the operators of a controlled network of computers, known as the "Nitol" botnet, and other malware, which, by means of numerous sub-domains of 3322.org, have and continue to cause irreparable injury to Microsoft, its customers, and the public.

PARTIES

2. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

3. Defendants Changzhou Bei Te Kang Mu Software Technology Co., Ltd., d/b/a Bitcomm, Ltd, (“Changzhou Bei Te Kang Mu Software Technology”), a Chinese corporation, and Defendant Peng Yong (“Mr. Yong”), an individual, are the names listed as the registrant of 3322.org, an Internet domain. Microsoft is informed and believes, and thereupon alleges that Mr. Yong, at all relevant times, was and is the owner, principal, agent, employee, or alter ego of Changzhou Bei Te Kang Mu Software Technology, doing the things herein alleged as both an individual and/or within the course and within the scope of such agency, including in his capacity as a principal, agent, employee and/or the alter ego of Changzhou Bei Te Kang Mu Software Technology. On information and belief, Defendant Peng Yong is the owner of Changzhou Bei Te Kang Mu Software Technology. Microsoft is informed and believes and thereupon alleges that Changzhou Bei Te Kang Mu Software Technology and Mr. Yong, through the 3322.org domain, provide critical support to the illegal Nitol botnet and other malware schemes.

4. Microsoft is informed and believes and thereupon alleges that John Doe 1 has established and operates the Nitol botnet using Nitol Variant A.

5. Microsoft is informed and believes and thereupon alleges that John Doe 2 has established and operates the Nitol botnet using Nitol Variant B.

6. Microsoft is informed and believes and thereupon alleges that John Doe 3 has established and operates the Nitol botnet using Nitol Variant C.

7. Microsoft is unaware of the true names or capacities of the Doe Defendants sued herein as John Does 1-3, and therefore sues these Doe defendants by such fictitious names. Microsoft will amend this complaint to allege the Doe Defendants’ true names and capacities when ascertained. Microsoft will exercise due diligence to determine Doe Defendants’ true

names, capacities, and contact information, and to effect service upon those Doe Defendants. Microsoft is informed and believes and therefore alleges that each of the fictitiously named Doe Defendants is responsible in some manner for the occurrences herein alleged, and that Microsoft's injuries as herein alleged were proximately caused by such Doe Defendants

8. Third Party Public Interest Registry ("PIR") is the domain registry that oversees the registration of all domains ending in ".org," including 3322.org, and is located at 1775 Wiehle Avenue, Suite 200, Reston, VA 20190.

9. The actions and omissions alleged herein to have been undertaken by the Defendants were undertaken by each Defendant individually, were actions and omissions that each Defendant authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of the Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance and benefited from those actions and omissions, in whole or in part. Each of the Defendants was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendants.

JURISDICTION AND VENUE

10. This action arises out of Defendants' violation of the Federal Computer Fraud and Abuse Act (18 U.S.C. § 1030). Therefore, the Court has subject matter jurisdiction of this action based on 28 U.S.C. § 1331. This is also an action for trespass to chattels, unjust enrichment, and negligence. Accordingly, this Court has subject matter jurisdiction under 28 U.S.C. § 1367.

11. Defendants have directed actions at Virginia, including the Eastern District of Virginia, by directing malicious computer code at the computers of individual users located in Virginia and the Eastern District of Virginia, specifically Fairfax, Virginia, infecting those user computers with the malicious code and thereby making the user computers part of the "botnet,"

which is used to injure Microsoft, its customers and the public.

12. Defendants have undertaken the foregoing acts with knowledge that such acts would cause harm through user computers located in Virginia, thereby injuring Microsoft, its customers, and others both in Virginia and elsewhere in the United States. Therefore, this Court has personal jurisdiction over the Defendants.

13. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district. A substantial part of the events or omissions giving rise to Microsoft's claims, occurred in this judicial district and a substantial portion of the property and individuals harmed through such acts are located in this district. Venue is proper in this judicial district under 28 U.S.C. § 1391(b) because a domain name is deemed to have its situs in the judicial district in which the domain name registry that registered or assigned the domain name is located. Non-defendant third – party PIR is the domain name registry for the .org top level domain, under which 3322.org is registered, and is located in this district. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because the Defendants are subject to personal jurisdiction in this judicial district.

FACTUAL BACKGROUND

Overview

14. This case began as a study into whether criminal organizations were exploiting the unsecure supply chain associated with the sale and distribution of counterfeit versions of Microsoft operating system software. Ultimately, however, Microsoft's investigation led to a major hub of illegal activity on the Internet causing great harm to consumers around the globe. Microsoft now has the opportunity to severely disrupt that illegal activity.

15. To provide a brief overview, as part of a global study into ways cyber criminals are infecting peoples' computers with malware, Microsoft researchers acquired and analyzed twenty new computers to see which, if any, had counterfeit versions of the Windows operating system installed on them. Very early on in the analysis, the researchers realized that one of the computers came not only preinstalled with counterfeit Windows, but also pre-infected with a

major variant of malicious software (“malware”) referred to as “Nitol.”

16. Upon returning to the United States, the research subsequently turned into an investigation of the Nitol malware specifically, ultimately leading Microsoft’s Digital Crimes Unit investigators to a provider of Internet services in China, Changzhou Bei Te Kang Mu Software Technology, and its owner Peng Yong, which run numerous websites, including one known as “3322.org.” The 3322.org domain provides supporting infrastructure for Nitol. The further investigation of 3322.org revealed that it provides a sprawling infrastructure supporting not only Nitol, but also a wide array of other illicit malware-related activities. These illegal activities include distribution and support for malware that can secretly record every keystroke a person makes at his or her keyboard; remotely steal passwords, financial data, and banking credentials; generate waves of spam; launch crippling attacks on other computers connected to the Internet; and even surreptitiously turn on a computer’s video camera and audio functions without the owner’s knowledge, to name just a few. In short, 3322.org is a major hub of illegal Internet activity, used by criminals every minute of every day to pump malware and instructions to the computers of innocent people world-wide.

Investigation Uncovers Connection between Counterfeit Windows Software and Nitol Botnet

17. In August, 2011, a team of forensic experts, working in China, purchased twenty new computers through typical retail channels to conduct a study into whether criminal organizations were exploiting the unsecure supply chain associated with the sale and distribution of counterfeit versions of Microsoft operating system software. They set the computers up in a rented private residence equipped with an Internet connection and began their analysis. They quickly determined that some of the computers came preinstalled not only with counterfeit versions of Windows, but also with some other pieces of malicious code.

18. The situation, however, quickly grew more alarming. In observing the computer infected with Nitol, the Microsoft investigators saw that it was engaging in highly unusual Internet activity. As soon as they powered on this particular computer, of its own accord and

without any instruction from the investigators, it began reaching out across the Internet, attempting to contact an unfamiliar computer. This is not standard Windows behavior. It is, however, classic behavior of a computer infected with malware. Many types of malware are programmed to connect to other computers on the Internet on start-up to download instructions or additional code, or to upload data.

19. Upon inspection of the computer pre-installed with counterfeit Windows software, the Microsoft investigators determined that the Nitol infection of this new machine was a result of purposeful or careless Windows installation. The investigators also observed that this Nitol infection was particularly virulent: it immediately copied itself to a thumb-drive inserted into the computer and from there copied itself onto another computer into which the thumb-drive was subsequently inserted. From past investigations, Microsoft investigators knew that spreading malware through removable media such as thumb drives is a classic infection strategy used by those who write and distribute malware. It spreads easily among innocent, unsuspecting people through their daily interaction between one another through their computers, even breaching the security of otherwise well-defended networks. Through further analysis of the malware, the Microsoft investigators identified it as a variant of malware known to Microsoft and others in the computer-security community as “Nitol.”

20. Ultimately, the investigators determined that three of the other computers with counterfeit versions of Windows were also infected with different types of malware. However that malware did not appear to be active. Accordingly, they focused their investigation on Nitol, which was highly active.

Nitol Is A Botnet

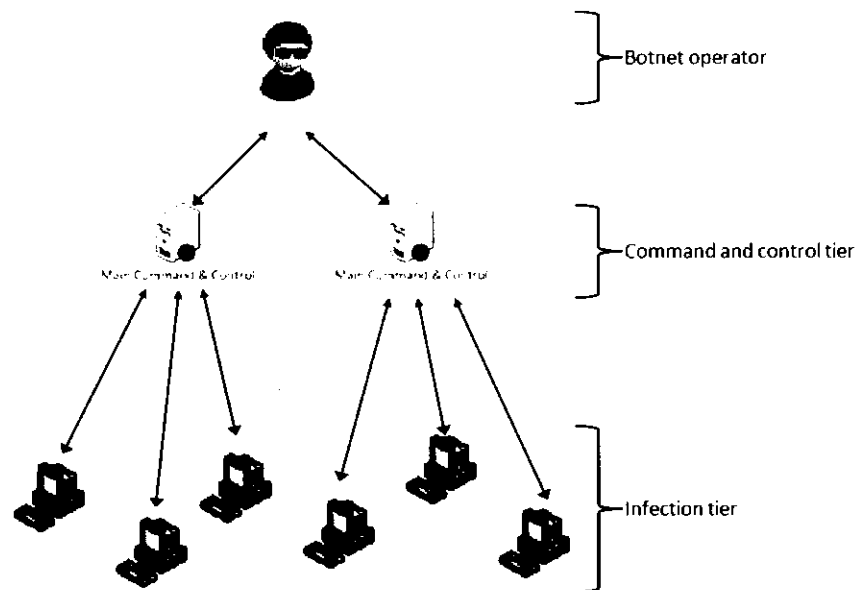
21. When a computer is infected with Nitol, it becomes part of a Nitol “botnet.” A botnet is a collection of individual computers, each running software that allows communication to other computers typically referred to as “command-and-control computers.” Command-and-control computers provide instructions or additional malware modules to the infected personal

computers and upload data from them. Malicious and criminal actors often use botnets because of their ability to support a wide range of illegal conduct, their resilience against attempts to disable them, and their ability to conceal the identities of the malefactors controlling them.

22. Botnets provide a very efficient means of controlling large numbers of computers and targeting any action internally against the contents of those computers or externally against other computers on the Internet. The third parties running the botnet (the “botnet operators”) can use the network of infected personal computers for various nefarious and criminal activities including spam, denial of service attacks on other computers connected to the Internet, theft of financial and banking data, eavesdropping, stalking, and other schemes. Access to the compromised personal computers can also be sold, leased, or swapped by one criminal group to another.

23. Microsoft has carefully studied the Nitol botnet architecture, design, and functions. As is typical of botnets, Nitol botnet operators organize their networks of computers into two-tier hierarchies, in which computers in each tier perform specific roles. Security experts refer to the lowest tier of the hierarchy as the “infection-tier.” The infection tier is comprised of infected personal computers owned by innocent and unsuspecting people. These might be office or home desktop computers, laptop computers, computers in public libraries, and so forth. These computers become infected in a variety of ways. A person may, for example, inadvertently interact with a website on which a malware downloader is staged; open an infected email attachment; download a fraudulent software product that contains the malicious botnet code; borrow an infected thumb-drive from a friend, colleague, or relative; or, as investigators saw in China, purchase a computer with counterfeit software pre-infected with Nitol. The malicious code infecting the person’s computer makes it part of the botnet. The spread of Nitol in this way is not related to any vulnerability in Microsoft’s systems, but is instead achieved by misleading people into taking steps that result in the infection of their computers, or, by misleading people into believing their new computer is free from infections and viruses. Once part of a Nitol botnet, the botnet controllers can now control the person’s computer.

24. The second tier is referred to as the “command-and-control tier.” The computers in the command-and-control tier communicate with the personal computers in the infection-tier, receiving information from them (e.g., stolen financial credentials), and sending instructions or new malware modules to them. Usually the number of command-and-control servers is small relative to the number of infected personal computers in the infection tier. The general structure of a Nitol botnet is depicted in the figure below.



25. Microsoft has detected nearly 4000 instances of Windows computers infected with some version of Nitol malware. This likely represents only a small subset of the number of infected computers. Microsoft’s data indicates that defendants have directed Nitol infections at computers located in Virginia, and in particular in Fairfax, in the Eastern District of Virginia, as well as other states.

Nitol Hijacks Processes Running on the Person’s Computer

26. Nitol harms Microsoft customers in a variety of ways. First, Nitol hijacks processes executing on personal computers. Nitol is selective about where it copies itself to the drives. It picks directories that contain applications (.EXE, .DLL, .OCX files) and compressed

file archives (e.g. .RAR and .ZIP). The reason Nitol copies itself to directories containing applications (e.g. files with extensions .EXE mainly) is to exploit the module loading process used by Windows when it runs applications. Applications are usually made up of many files. These files are usually organized in different folders beneath a main directory.

27. When started, one of the first things an application does is to request that Windows load into the computer's memory the several different types of files the application needs to run. Some of these files contain code that the application uses. These code-carrying files are called dynamic link libraries and they typically have the file extension ".DLL." When an application is started and requests that Windows load the necessary files, Windows will attempt to find the files (on the application's behalf) in the application's directory first. If a copy of the needed file is not found, Windows then searches several other places in a well-known protocol, and then the process ends with a search for the needed file in the Windows system directories.

28. Nitol's filename is called "LPK.DLL." Upon information and belief, the authors of Nitol chose this name because Windows contains a legitimate file that is also named LPK.DLL. The real Windows version of LPK.DLL is loaded by almost any application that has a graphical user interface, and even some that do not. The official versions of LPK.DLL are located in Windows system file folders that are installed as part of Windows. On an uninfected machine, when an application starts up, Windows will look for LPK.DLL first in the application's own folder, and failing to find it there, will ultimately load an official version from a Windows directory. Since applications look for LPK.DLL in their current directory before any other place Nitol will get loaded before the legitimate file (of the same name) provided by Microsoft in the Windows directory. Consequently, by usurping the file name "LPK.DLL," Nitol is capable of hijacking almost any application running on the person's computer.

29. Microsoft's research indicates that customers have accessed files on their computers which were infected with Nitol hundreds of thousands of times. The scale of this access represents an overwhelming risk that the botnet files will be spread and botnet will grow,

compounding the damage.

Nitol Can Breach Security Between People's Computers

30. Nitol infects people's computers through a variety of common mechanisms, but it mainly spreads through removable media such as flash drives, zip/rar files, and the like. Once infected with Nitol a computer will copy the virus to all drives attached to the system. This includes USB drives, external hard disks, and even company/corporate network servers and shared drives that are mapped to the system.

31. Spreading Nitol is simple to do using this mechanism as it means Nitol does not need to trick the person into running an application for infection to occur. Instead, the Nitol LPK.DLL file merely needs to get copied to a directory that contains an application the person is likely to use. After Nitol copies LPK.DLL to a removable disk (its main infection mechanism), any person that runs an application from that disk will infect the computer on which they run the application; e.g. laptop, home, work, or public kiosk machine.

32. This also means that Nitol can bridge network boundaries and security mechanisms because people typically carry setup programs, application patches, and other software between home and work using removable storage devices, and people often use thumb-drives to share files with one another. All of these are vulnerable to this type of infection mechanism.

Nitol Can Enlist The Person's Computer In Illegal Attacks On Other Computers

33. Microsoft's forensic analysis of Nitol shows that it can enlist the person's computer in illegal attacks on other computers connected to the Internet. There are three major versions of Nitol, which Microsoft security investigators refer to as Nitol.A, Nitol.B, and Nitol.C (the latter being the newest version discovered late 2012, revealing the growing threat that Nitol presents). All versions are very similar and each fall within categories of malware referred to as "rootkits" and "backdoors." The term "rootkit" refers to a type of malware that gains a privileged level of access to a computer and which reconfigures the system to conceal itself. The

term “backdoor” refers to malware that opens a secret channel of communication with a third-party on the Internet, which gives that third party surreptitious and remote control over the computer. In the case of Nitol, that third-party is the botnet operator.

34. Nitol runs as a background process (that is, it runs in the background, has no user-interface, and gives the computer’s owner no indication that it is present or running) and performs the commands sent from an attacker. Microsoft investigators reverse-engineered the Nitol.A sample that they acquired in China and studied its functionality to determine what commands it is capable of executing. They compared this with the functionality of Nitol.B and determined the commands to be the same. The table below shows the commands and functionality that is made available to botnet operators through Nitol.

C&C Command ID	Action	Threat
0x01 (1)	Receive Component	Send a new module to the computer to run.
0x02 (2)	Unknown but DDOS Specific	<ul style="list-style-type: none"> Nitol connects to target address via TCP, UDP, or RAW. Possible floods: SYN, TCP, UDP, ICMP, HTTP. C&C may command sleep for specific time.
0x03 (3)	Unknown but DDOS Specific	
0x04 (4)	Unknown but DDOS Specific	
0x05 (5)	Stop Work	Stop DDOS’ing target computers
0x06 (6)	Clean up	Delete, set file attributes to Normal. Exits.
0x10 (16)	Download & Run	<ul style="list-style-type: none"> Specify URL and filename to download from Internet Save file in temp directory under filename “stf[5 random letters].exe” Executes saved file
0x12 (18)	Update	<ul style="list-style-type: none"> Delete existing service Download new executable from specified URL Save file in temp directory under filename “stf[5 random letters].exe” Execute saved file
0x13 (19)	Open URL	Launch Internet Explorer (specifically) with specified URL
0x14 (20)	Open URL as Current User	Launch Internet Explorer (specifically) with specified URL
0x20 (32)	Start Work	Start DDOS’ing target computers
0x77 (119)	Get Computer Information	<ul style="list-style-type: none"> Get computer information and send to C&C <ul style="list-style-type: none"> Computer Local (e.g. EN-US) Computer Name

		<ul style="list-style-type: none"> ○ Operating System Name ○ Amount of memory (RAM) ○ CPU Speed ○ Nitol Flag (possibly version number) ○ Nitol Work DLL flag ○ Timestamp
--	--	--

35. These commands indicate that Nitol is designed to enlist whatever computer it infects into distributed denial of service (“DDOS”) attacks. A DDOS attack occurs when large numbers of computers on the Internet are directed to attack the services of other computers on the Internet. For example, if the computers of several hundred thousand people are infected, these computers can be directed to simultaneously request a communication connection to a business’s website, the sheer volume of attempted connections may overwhelm the business’s system and render the business’s website unavailable to any legitimate user and may cause other damage as well. DDOS attacks, and even the threat of such attacks, can and have been used to retaliate against, blackmail, or to silence companies, private organizations, and governments.

36. Microsoft’s reverse engineering of Nitol shows that it comes with a full complement of commands needed to direct an infected personal computer to connect to a target computer and flood it using a variety of communications means. In the table above, commands 0x02 (2), 0x03 (3), 0x04 (4), 0x05 (5), and 0x20 (32) provide functionality in support of DDOS attacks. Nitol.B samples analyzed by Microsoft for network behavior have been seen to perform DDOS attacks. Most network traffic analyzed thus far suggests the infected computers are active but awaiting instructions. Other infected computers are deliberately flooding web sites with so much network traffic using DDOS attacks, that legitimate users cannot patronize the online business.

Nitol Opens A Backdoor On The Person’s Computer
Allowing Access To And Control By Criminals

37. Microsoft’s forensic analysis also shows that Nitol opens a backdoor on a person’s computer allowing access to and control by criminals. The commands shown in the

table above indicate that Nitol is capable of downloading, installing, and running additional software modules. In other words, Nitol provides an extensible platform for other malware. It is designed to provide a framework into which other malware modules can be plugged. For example, there may be a specialized malware module designed to steal passwords, another to commit click fraud, another to steal banking credentials, and another to send spam.

38. Nitol is designed to download and execute these additional software modules. Thus, Nitol is an open framework and appears to be one that is likely sold as a kit or source code project. Because of its extensible nature, access to a computer that is infected with Nitol can be leased, sold or traded among criminal groups gathering together networks of infected computers for varying purposes. In the table above, commands 0x01 (1), 0x10 (16), and 0x12 (18) are related to downloading and installing additional modules. This feature makes Nitol a backdoor and allows the botnet operator to do at least as much on the victim's computer as the victim can.

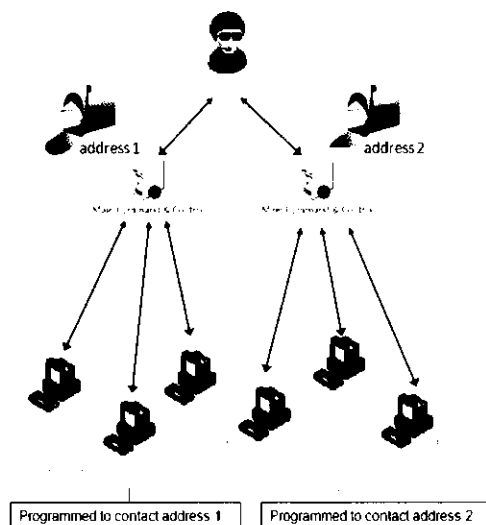
Microsoft Customers Need To Expend Considerable Time Combating Nitol Infections

39. Most if not all owners of Nitol-infected computers are unaware that their machines are infected and operating as part of a Nitol botnet, or that their computers are secretly engaged in illegal activity directed against the computer's owner, or against other computers connected to the Internet. This is in part because the Nitol malware that infects a person's computer conceals itself by changing the Windows settings related to Nitol files so that they remain hidden. In particular, Windows has settings for normal files, "hidden files," and "super hidden files." Nitol configures the person's computer so that Nitol files are "super hidden."

40. Numerous software providers and software security firms are constantly engaged in trying to disinfect computers. That, however, is a complex task. Because Nitol hides itself, owners of infected computers need to perform advanced steps to even become aware of the infection, something many consumers are unable to undertake independently. Also, the Nitol infection protects itself by replacing malicious files on the user's hard drive if they are ever deleted.

**Nitol Command-And-Control Infrastructure: Nitol Is
Controlled By The Domain 3322.org**

41. The Nitol malware on infected computers are programmed to connect to a command and control domain name, as represented in the following figure. As already described, such infected computers will reach out over the Internet to the command and control domain, without the owner's permission or knowledge, from which they will download additional malicious software and instructions from third parties, who now effectively control the operation of the innocent owner's computer.

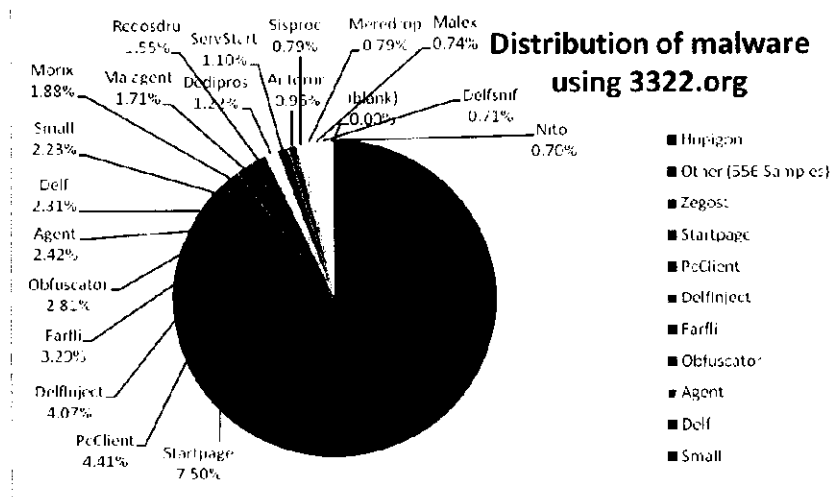


42. After identifying Nitol malware loaded on the computer with the counterfeit operating system, Microsoft investigators set about investigating the connections that Nitol-infected personal computers try to make to other computers on the Internet. To do this, they studied 2200 samples of Nitol malware. The Nitol samples obtained by Microsoft all connect to command-and-control servers via a domain called "3322.org." In particular, the infected computers reach out to specific "sub-domains" of 3322.org (for example, "illegal.3322.org").

43. Each such 3322.org sub-domain is associated with an IP address. Microsoft began tracking Nitol.A in February 2011 and observing the location of such IP addresses. Early detections originated in China, indicating that the Nitol family of malware started in China. The growth rate of infections since this date suggests that the virus started being widely distributed in

2011. Microsoft's investigation reveals that China is by far the country with the largest number of Nitel command-and-control servers (mostly in Beijing), followed by the United States and the Cayman Islands—all of which are contacted through 3322.org.

44. A further analysis of 3322.org showed that 3322.org is functioning as hub for many other varieties of malware circulating on the Internet. The figure below shows the diversity of malware that is controlled from 3322.org, each a threat to Microsoft.



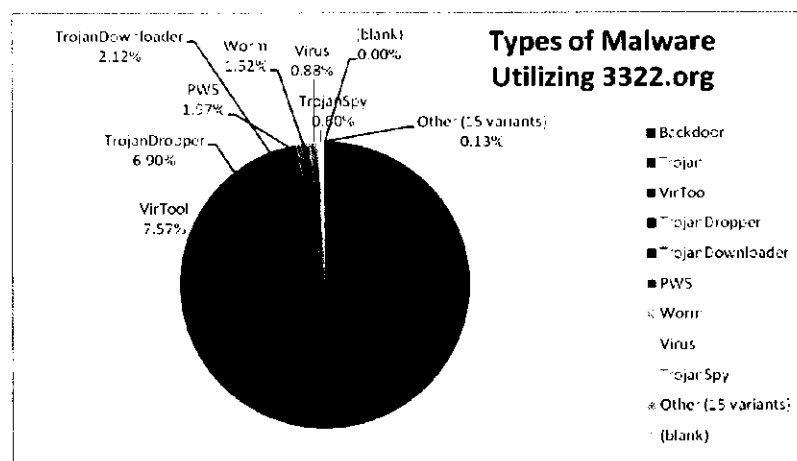
45. Through 3322.org and its sub-domains, a very large number of small, transient websites are provided a continuous Internet presence. For example, malware on a person's infected computer might be programmed to contact "virus.3322.org." The person's computer would first contact 3322.org to get the address of the "virus" sub-domain, and 3322.org would direct it onward. This type of system provides a low cost way for transient websites that move from IP address to IP address to provide a stable domain name for malware infected computers to contact. In the example above, the virus.3322.org sub-domain can operate from a changing set of IP addresses. As long as that sub-domain updates 3322.org as to its current IP address, malware infected machines attempting to reach it will always be able to do so.

46. This type of service is an ideal structure to support and monetize cybercrime activities, given the speed with which sub-domains can change. This fact is evident from the massive number of Nitel and other malware command and control servers contained on

3322.org. By studying thousands of samples of malware, Microsoft has been able to identify approximately 70,000 sub-domains of 3322.org that are supporting malware infections, and there are likely many more. Other researchers have observed the same. For example, one security research firm reported that in a single year, 3322.org accounted for 17.41% of the world's malicious URL transactions. Another security researcher reported that 40% of all malware programs, at one point or another, connected to 3322.org. The great variety and quantity of malware using 3322.org as infrastructure is testament to the utility of this kind of system for those engaged in illegal Internet activities. The top six types of malware currently using 3322.org are described in the table below.

Malware	Purpose
Hupigon	Allows a remote attacker to control a victim's web camera, microphone, take screen shots, and copy/delete user files on the infected computer.
Zegost	Connects to a command-and-control server to receive instructions capable of executing any behavior the attacker wants.
StartPage	Hijack's user's browser by changes a victim's Internet Browser home page w/o consent.
PcClient	Family of Trojan malware with several components including key logger, backdoor, and a rootkit.
DelfInject	Copies and installs software on victim's computer. Commonly installing a remote backdoor which allows an attacker surreptitious access to infected systems.
Farfli	Typically directs victims to web sites not of their choosing. Also has backdoor capabilities that allow it to connect to remote attacker and await for instructions.

47. The following figure shows the distribution by category of the malware controlled by 3322.org.



48. These categories are explained in the following table.

Malware Type	Purpose
Backdoor	Allows an attacker to perform at least the same activity as the user that is compromised. This includes turning on web camera and eaves dropping via microphone, taking screenshots, copying/moving/deleting files on the user's system, and keystroke logging.
Trojan	Packaged as legitimate software, this malware contains code to compromise a victim's computer by installing one of the other listed types of additional malware.
Virus tool	Generic classification given to applications that are primarily used to create, obfuscate, or facilitate the making or distribution of malware
Trojan Dropper	An application whose sole purpose is to download and execute software on a victim's computer. Also used to denote an application that is downloaded and executed on a victim's computer.
Trojan Downloader	An application whose sole purpose is to download files onto a victim's computer. Also used to denote an application that is copied to a victim's computer.
PWS	Password Stealer. This type of malware logs user keystrokes or retrieves text typed by the user with the sole purpose of obtain user credentials.
Remote Access	An application that allows remote connections to a victim's computer. This program, once run on a computer, allows visual/keyboard/mouse/audio control over victim's computer.
Browser Modifier	Typically a web site or denotes an application that replaces search results, URL navigation, WPAD or DNS resolution, and/or click information with destinations of the attacker's choosing.

Irreparable Harm To Microsoft And Customers From Nitel And 3322.org

49. Microsoft is the provider of the Windows operating system and a variety of other software and services. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Windows marks.

50. The activities of Nitol and other malware on 3322.org injure Microsoft and its reputation, brand, and goodwill because users subject to the negative effects of these malicious applications incorrectly believe that Microsoft or Windows is the source of their computer problems. Additionally, Microsoft devotes significant computing and human resources to combating Nitol and other malware infections and helping customers determine whether or not their computers are infected, and if so, cleaning them. Customers' frustration with having to deal with Nitol and other malware infections on their computers diminishes their regard for Windows and Microsoft, and tarnishes Microsoft's reputation and goodwill.

51. Once customers' computers are infected and become part of the Nitol botnet or infected by other malware controlled through 3322.org, they may be unaware of that fact and may not have the technical resources to solve the problem, allowing their computers to be misused indefinitely. This is particularly true for Nitol given its ability to conceal and protect itself. In such circumstances, technical attempts to remedy the problem may be insufficient and the injury caused to customers will continue. The injury caused by the Nitol botnet and 3322.org extends far beyond Microsoft to other consumers and providers, into internet infrastructure and ultimately to the majority of computer users worldwide, placing each at increased risk.

52. Further, customers may incorrectly attribute the negative impact of the Nitol botnet and other malware controlled through 3322.org to Microsoft. Additionally, there is a serious risk that customers may move from Microsoft's products and services because of such activities. And, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks.

53. Microsoft and its customers are injured when the Nitol botnet software and other malware controlled through 3322.org is maliciously introduced onto people's computers making them part of the botnet. The installation of the botnet software by deceiving consumers and without Microsoft's authorization is an intrusion into the Microsoft Windows operating system (which is licensed to Microsoft's customers), without Microsoft's authorization.

54. The Nitol botnet and other malware controlled through 3322.org installs and runs

software without the customers' or Microsoft's knowledge or consent. The Nitol botnet specifically targets the Windows operating system. For example, it mimics particular files that are specific to the Windows operating system, without the consent of Microsoft or its customers.

55. Once part of the botnet, the person's computer is under control of the parties controlling the botnet. The operators of the botnet can use the victim's computer and the code for any number of malicious purposes, such as stealing personal information stored on the system, sending bulk, unsolicited "spam" emails, delivering malicious software to infect other computers or otherwise using it to carry out fraud, computer intrusions or other malicious and illegal conduct. Once the person's computer is under the control of the parties controlling the botnet, the computer's performance may suffer due to the repeated copying of files, data transfer and connections to the Internet that the botnet causes the person's computer to undertake without the person's permission.

56. The Nitol botnet is designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. For example, the Nitol command and control system can be leveraged to update the malware to point to a different command and control sub-domain within milliseconds of Defendant's notice.

57. Piecemeal requests to turn off the domains, informal dispute resolution or notice to the Defendants prior to turning off the command and control domains would be insufficient to curb the injury. The botnet will very likely be moved and hidden if notice were given before turning off these domains. The parties controlling the botnet have built in mechanisms designed to permit the Nitol botnet to continuously change location and to obfuscate its operations. In other instances where security researchers or the government attempted to curb injury caused by botnets, but allowed the botnet operators to receive notice, the botnet operators immediately moved the botnet to new, unidentified locations and took other countermeasures causing the botnet to continue its operations and destroying or concealing evidence of the botnet's operations. Given the specific architecture of the Nitol botnet's command and control sub-domains on 3322.org, it is very likely that the operators of the Nitol botnet would update infected

installations with new (and different) primary command and control domain names. Defendants controlling 3322.org have not been cooperative in the past regarding the malicious activity emanating from the domain, and such has continued and grown rapidly.

58. Infection rates for Nitol A and B have likely peaked. This suggests that the operators of Nitol may be moving from a phase in which they have been focused on infecting computers with Nitol to a phase in which they are focused on monetizing their networks of infected personal computers through increased illegal activity

FIRST CLAIM FOR RELIEF

(Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

59. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 58 above.

60. Defendants: (a) knowingly and intentionally accessed Microsoft customers' protected computers and Microsoft's protected computers without authorization or in excess of any authorization and thereby obtained information from the protected computers in a transaction involving an interstate or foreign communication (18 U.S.C. § 1030(a)(2)(C)), (b) knowingly and with an intent to defraud accessed the protected computers without authorization or in excess of any authorization and obtained information from the computers, which Defendants used to further the fraud and obtain something of value (18 U.S.C. § 1030(a)(4)); (c) knowingly caused the transmission of a program, information, code and commands, and as a result of such conduct intentionally caused damage without authorization to the protected computers (18 U.S.C. § 1030(a)(5)(A)); and/or (d) intentionally accessed the protected computers without authorization, and as a result of such conduct caused damage and loss (18 U.S.C. § 1030(a)(5)(C)).

61. Defendants' conduct has caused a loss to Microsoft during a one-year period aggregating at least \$5,000.

62. Microsoft has suffered damages resulting from Defendants' conduct.

63. Microsoft seeks compensatory and punitive damages under 18 U.S.C. § 1030(g) in an amount to be proven at trial.

64. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SECOND CLAIM FOR RELIEF
(Common Law Trespass to Chattels)

65. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 58 above.

66. Defendants' actions in operating the Nitel Botnet result in unauthorized access to the computers of Microsoft and its customers and result harm to those computers.

67. Defendants intentionally caused this conduct and this conduct was unauthorized.

68. Defendants' actions have caused injury to Microsoft and its customers and imposed costs on Microsoft and its customers, including time, money and a burden on the computers of Microsoft and its customers, as well as injury to Microsoft's business goodwill and diminished the value of Microsoft's possessory interest in its computers and software.

69. As a result of Defendants' unauthorized and intentional conduct, Microsoft has been damaged in an amount to be proven at trial.

70. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

THIRD CLAIM FOR RELIEF
(Common Law Conversion)

71. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 58 above.

72. Defendants have willfully interfered with and converted Microsoft's personal property, without lawful justification, as a result of which Microsoft has been deprived of possession and use of its property.

73. As a result of Defendants' actions, Microsoft has been damaged in an amount to be proven at trial.

74. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FOURTH CLAIM FOR RELIEF
(Unjust Enrichment)

75. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 58 above.

76. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at Microsoft's expense in violation of the common law.

77. Defendants accessed, without authorization, computers running Microsoft's software.

78. Defendants profited unjustly from their unauthorized and unlicensed use of Microsoft's software and the computers of Microsoft and its customers.

79. Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's software and the computers of Microsoft and its customers.

80. Retention by the Defendants of the profits they derived from their unauthorized and unlicensed use of Microsoft's software and the computers of Microsoft and its customers would be inequitable.

81. Defendants' unauthorized and unlicensed use of Microsoft's software and use of the computers of Microsoft and its customers have damaged Microsoft in an amount to be proven at trial, and Defendants should disgorge their ill-gotten profits.

82. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FIFTH CLAIM FOR RELIEF

(Negligence)

83. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 58 above.

84. The Defendants were and are subject to a duty to exercise care to prevent their own use or any third party's use of domains to control the Nitol botnet and to engage in the malicious conduct alleged in this complaint. The source of such duty of care includes, but is not limited to, Defendants' contractual obligations not to use or allow use of the domains for the purposes and acts alleged herein, as set forth in the domain registration agreements and policies entered into by Defendants, including the Cloud Group Ltd. domain registration agreements set forth at Appendices B-C to this Complaint.

85. The Defendants breached that duty of care by registering sub-domains that are used to control the Nitol botnet and using or allowing their licensee customers to use the 3322.org sub-domains to control the Nitol botnet and to engage in the malicious conduct set forth herein.

86. The Defendants' breaches of that duty of care as set forth above have actually and proximately caused Microsoft to suffer and to continue to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

87. As an actual and proximate result of the Defendants' breach of their duty of care,

Microsoft is entitled of damages to be proven at trial.

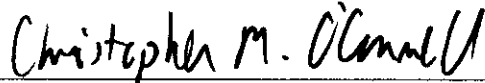
PRAYER FOR RELIEF

WHEREFORE, Plaintiff Microsoft prays that the Court:

- A. Enter judgment in favor of Microsoft and against the Defendants;
- B. Declare that Defendants conduct has been willful and that Defendants have acted with fraud, malice and oppression;
- C. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;
- D. Enter judgment awarding Microsoft actual damages from Defendants adequate to compensate Microsoft for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial;
- E. Enter judgment disgorging Defendants' profits.
- F. Enter judgment awarding enhanced, exemplary and special damages, in an amount to be proved at trial;
- G. Enter judgment awarding attorneys' fees and costs; and
- F. Order such other relief that the Court deems just and reasonable.

Dated: September 10, 2012 Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP



REBECCA L. MROZ

Va. State Bar No. 77114

CHRISTOPHER M. O'CONNELL

Va. State Bar No. 65790

Attorneys for Plaintiff Microsoft Corp.

ORRICK, HERRINGTON & SUTCLIFFE LLP

Columbia Center

1152 15th Street, N.W.

Washington, D.C. 20005-1706

Telephone: (202) 339-8400

Facsimile: (202) 339-8500

bmroz@orrick.com

coconnell@orrick.com

Of counsel:

GABRIEL M. RAMSEY (pro hac vice application pending)

Attorneys for Plaintiff Microsoft Corp.

ORRICK, HERRINGTON & SUTCLIFFE LLP

1000 Marsh Road

Menlo Park, CA 94025

Telephone: (650) 614-7400

Facsimile: (650) 614-7401

gramsey@orrick.com

JEFFREY COX (pro hac vice application pending)

Attorneys for Plaintiff Microsoft Corp.

ORRICK, HERRINGTON & SUTCLIFFE LLP

701 Fifth Avenue

Suite 5600

Seattle, WA 98104-7097

Telephone: (206) 839-4416

Facsimile: (206) 839-4301

jcox@orrick.com